UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/483,164 | 01/14/2000 | Daniel Jay Thomsen | 105.174US1 | 8029 |

21186 7590 11/15/2005

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH
1600 TCF TOWER
121 SOUTH EIGHT STREET
MINNEAPOLIS, MN 55402

| EXAMINER | |
|---|---|
| SIMITOSKI, MICHAEL J | |
| **ART UNIT** | **PAPER NUMBER** |
| 2134 | |

DATE MAILED: 11/15/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 09/483,164 | THOMSEN ET AL. | |
| | Examiner | Art Unit | |
| | Michael J. Simitoski | 2134 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *23 September 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-35* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-35* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *14 January 2000* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

## DETAILED ACTION

1. The response of 9/23/2005 was received and considered.

2. Claims 1-35 are pending.

### *Response to Arguments*

3. Applicant's arguments filed 9/23/2005 have been fully considered but they are not persuasive.

4. Applicant's response (p. 9, ¶3-6) argues that claims 6-11 are directed to a machine which produces a useful, concrete and tangible result. In light of Applicant's amendments to the claims, the rejections of claims 1-5 & 14-35 under 35 U.S.C. §101, set forth in the previous Office Action, are withdrawn. The rejection of claims 6-13 under §101 is maintained. There is no recitation of "machine" in claims 6-13, but rather a system. Assuming the useful, concrete and tangible result that the claimed system is reciting is a translated security policy, there is no recitation in the claims that the translation is performed by a machine.

5. The amendments to claims 12-13 overcome the previous §112 ¶2 rejection on those claims and therefore the rejection is withdrawn.

6. Applicant's response (p. 10 – p. 11, ¶4) argues that Thomsen does not consider or mention the user of semantic layers to combine keys into key chains and that the layers of Thomsen are not used to combine keys into key chains and then to encapsulate chains as keys before passing the new keys to a different semantic layer. Further, Applicant argues that Thomsen does not describe encapsulating key chains as keys within a semantic layer or passing the encapsulated chains to the next semantic layer. However, as previously described Thomsen

discloses semantic layers (§1, ¶1 & Fig. 1) to combine keys into key chains (Fig. 1 & Fig. 2), encapsulating key chains (for example "Doctor" and "Nurse", Fig. 2) as keys ("Health Care Provider", Fig. 2) within a semantic layer (application) (Fig. 1) and passing the encapsulated key chains to the next semantic layer (enterprise) (Fig. 1, §2 ¶3 & §2.7). The purpose of encapsulating within the application layer and passing the encapsulated key chains to another semantic layer is to manage the encapsulated key chains as a single unit. Applicant notes that "Health Care Provider" actually has fewer permissions than either of the two keys that are the result of encapsulation. However, the claims do not recite that the encapsulated key chains have more permissions than a non-encapsulated key chain. Thomsen is combining (Fig. 2) the permission to getPrimaryPhysician, getBloodPressure and setBloodPressure that is contained in the Nurse and Doctor keys and creating a Health Care Provider key to be used at the next semantic layer (enterprise). Further, Thomsen combines the inheritable permissions of different types of doctors into a single "doctor" key. The keys are then exported to an enterprise layer in which they are combined and assigned to users (§2.6).

7. Applicant's response (p. 11, ¶3) argues that Thomsen does not describe the use of a plurality of semantic layers, wherein two or more of the semantic layers are used to encapsulate key chains as keys. It is noted that claims 1-5 & 32 do not recite this limitation, however this argument is applicable to claims 6-31 & 33-35. However, regarding claims 6-13, the claims only recite that keys are encapsulated at more than one layer, not specifically that keys from a first application policy layer are encapsulated and exported as keys to a second semantic policy layer, where they are encapsulated and exported to a third local policy layer, as per claims 14-31 & 33-35. Applicant's response (p. 11, ¶3) further argues that Thomsen does not describe a user

interface for defining a security policy as a function of keys received from a plurality of lower semantic layers. However, claims 6-10 do not recite defining a security policy as a function of keys received from a plurality of lower semantic layers, but recites doing so only from a single lower semantic layer. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). Therefore, the rejection of claims 1-13 & 32 in view of Thomsen is maintained. The rejections of claims 14-31 & 33-35 in view of Thomsen are withdrawn.

8. Applicant's response (p. 11, ¶6) argues that "Napoleon Network Application Policy Environment" does not qualify as prior art because the authors are included in the list of inventors of the instant application. However, as stated in §2132 of the MPEP,

> "Others" Means Any Combination of Authors or Inventors Different Than the Inventive Entity. The term "others" in 35 U.S.C. 102(a) refers to any entity which is different from the inventive entity. The entity need only differ by one person to be "by others." This holds true for all types of references eligible as prior art under 35 U.S.C. 102(a) including publications as well as public knowledge and use. Any other interpretation of 35 U.S.C. 102(a) "would negate the one year [grace] period afforded under § 102(b)." In re Katz, 687 F.2d 450, 215 USPQ 14 (CCPA 1982).

Because the instant invention's inventive entity includes a combination of authors different than the article authors (the instant inventive entity includes Bogle, who is not an author of the article), the article meets the requirement for 35 U.S.C. §102(a).

9. Applicant's response (p. 11, ¶7) argues that the non-patent literature reference to Sandhu does not qualify as prior art under §102(e). The Examiner apologizes for any confusion as this is a typographical error and is meant to say §102(a), under which Sandhu qualifies as prior art. Applicant's arguments against Sandhu will be discussed below.

10. Applicant's response (p. 12, ¶1) argues that Sandhu lacks encapsulating "security mechanism application specific information for each security mechanism". However, for each security mechanism/permission, security mechanism application specific information/application permissions are encapsulated into abilities (p. 122, §5). In accordance with applicant's definition (a security mechanism must be an abstract representation of rights associated with the security mechanism) which is what a "permission" is disclosed as in Sandhu. Sandhu's permissions are the rights to perform an action. Sandhu discloses the following concepts: (1) Permissions are encapsulated into abilities (which can contain other abilities), and (2) abilities are assigned, with users, to roles (which can contain other roles). Because roles can contain other roles, a layer exists to which roles are "combined" and exported. A semantic layer can be thought of as a particular layer abstracting permissions into abilities, a layer abstracting roles to different users, or some combination of the two. Therefore, Sandhu discloses encapsulating security mechanisms as keys (permissions), combining keys/permissions and exporting them as keys/abilities to another layer and combining keys/abilities to form key chains (abilities or UP-roles, both of which contain abilities) and exporting the key chains to another layer (one which uses RBAC UP-roles) (p. 122, ¶5).

11. Applicant's response (p. 12, ¶5) argues that Sandhu lacks key limitations. However, Sandhu has been discussed above.

12. Applicant's response (p. 12, ¶6) argues, regarding claims 6-10, that neither Sandhu nor Crall discloses "a plurality of semantic layers, including a first semantic layer, wherein the two or more semantic layers combine keys into key chains, encapsulate the key chains as keys and export the keys to another semantic layer, wherein each key encapsulates security mechanism

application specific information for a security mechanism". However, Sandhu discloses permissions being combined into abilities (keys) and abilities combined with other abilities for form new abilities (key chains) and encapsulating key chains/abilities as keys/abilities and passing the key chain keys/abilities to another semantic layer (UP-roles) (p. 122, §5). Further, because UP-roles can contain other UP-roles (UP-roles), there exists another semantic layer where UP-roles are encapsulated into a UP-role and exported (i.e. a first semantic layer containing UP-roles and a second semantic layer containing combined and encapsulated UP-roles from the first semantic layer) (p. 122, §5).

13. Applicant's response (p. 13, ¶2) argues that neither Sandhu nor Crall teach or suggest a security system having "a tool for manipulating the model, wherein the tool allows an administrator to: encapsulate security mechanism application specific information for a security mechanism, wherein encapsulating includes forming a key for each security mechanism; combine keys to form key chains; encapsulate key chains as keys within two or more semantic layers; pass the key chain keys to other semantic layers; form user key chains from the key chain keys; and associated users with the user key chains". However, as discussed above, Sandhu discloses permissions being combined into abilities (keys) and abilities combined with other abilities for form new abilities (key chains) and encapsulating key chains/abilities as keys/abilities and passing the key chain keys/abilities to another semantic layer (UP-roles) (p. 122, §5). Further, because UP-roles can contain other UP-roles (UP-roles), there exists another semantic layer where UP-roles are encapsulated into a UP-role and exported (i.e. a first semantic layer containing UP-roles and a second semantic layer containing combined and encapsulated UP-roles from the first semantic layer) (p. 122, §5).

14. Applicant's response (p. 13, ¶3) argues that neither Sandhu nor Crall teach or suggest encapsulating key chains as keys within two or more semantic layers as claimed in claims 14-31 and 33-35. This argument is persuasive with regard to claims 14-31 and 33-35 in that Sandhu fails to disclose encapsulating keys as key chains and exporting key chains as keys in an application policy layer, and a semantic policy layer and combining one or more keys in a local policy layer to form one or more local policy key chains.

### *Drawings*

15. New corrected drawings in compliance with 37 CFR 1.121(d) are required in this application because the drawings are handwritten (Figs. 1-3), have handwritten figure numbers and/or labels (Figs. 1-19), contain dark contrast (Figs. 4 & 11) and contain small objects which are difficult to read (Figs. 14-17 & 19). Applicant is advised to employ the services of a competent patent draftsperson outside the Office, as the U.S. Patent and Trademark Office no longer prepares new drawings. The corrected drawings are required in reply to the Office action to avoid abandonment of the application. The requirement for corrected drawings will not be held in abeyance.

### *Claim Rejections - 35 USC § 101*

16. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

17. Claims 6-13 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The invention of the claims is not tangibly embodied.

### *Claim Rejections - 35 USC § 112*

18. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

19. Claims 6-10 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. The specification does not describe how a "layer" can combine keys into key chains, etc., as a layer is an abstract idea.

20. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

21. Claims 6-13 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Regarding claims 6-10, the limitation "the two or more of the semantic layers" lacks antecedent basis.

Regarding claims 6-10, it is unclear how a "layer" can combine keys into key chains, etc., as a layer is an abstract idea.

Regarding claims 11-13, it is unclear whether "allows" (line 3) is to be interpreted, as "allows" simply describes the effect of the tool, rather than the structure or configuration. For the purpose of this action, "allows" is understood to mean "is configured to".

Regarding claims 11-13, "the key chain keys" (lines 10-11) lacks antecedent basis.

### *Claim Rejections - 35 USC § 102*

22. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

23. Claims 1-3, 5 & 11-13 are rejected under 35 U.S.C. 102(a) as being anticipated by printed publication "Role Based Access Control Framework for Network Enterprises" by Thomsen, O'Brien and Bogle (**Thomsen**).

Regarding claim 1, Thomsen discloses encapsulating security mechanism application specific information for each security mechanism/methods (Fig. 1 & §2.4), wherein encapsulating includes forming a key for each security mechanism (Fig. 2 & §2.4), combining keys to form key chains (Figs. 1 & 2), encapsulating key chains as keys (for example "Doctor" and "Nurse", Fig. 2) as keys ("Health Care Provider", Fig. 2) and passing the key chain keys to another semantic layer (from application to enterprise) (§2.5), defining the security policy, wherein defining includes forming key chains from keys and associating users with key chains (§2.6-§2.7), translating the security policy (p. 7, last ¶2) and exporting the translated security

policy to the security mechanisms (to CORBA using ADAGE (p. 8, ¶1) and enforcing the security policy via the security mechanisms/CORBA (p. 8, ¶1).

Regarding claim 2, Thomsen discloses a distributed computer network (§1.1).

Regarding claim 3, Thomsen discloses the security mechanisms being heterogeneous (p. 8, §3.2).

Regarding claim 5, Thomsen discloses defining the policy using a graphic user interface/NAPOLEAN policy tool (Fig. 4 & §3.1, "Specifying Policy").

Regarding claims 11 & 13, Thomsen discloses a model comprising semantic layers for defining different security policies and constraints for each type of user (Fig. 1), a tool for manipulating the model (§3), wherein the tool allows an administrator to encapsulate security mechanism application specific information for each security mechanism, wherein encapsulating includes forming a key for each security mechanism (Fig. 2), combine keys (primary physician, consulting physician) to form key chains (doctor) (§2.4), encapsulate key chains as key keys within two or more semantic layers (§2.4 and §2.6), pass the key chain keys to other semantic layers/doctor to other semantic layers/enterprise (§2.5-2.6), form user key chains from the key chain keys (§2.6 & Fig. 4) and associate users with the user key chains (§2.6) and a translator for translating security policies from the model to the security mechanisms in one or more computer resources (§3.1).

Regarding claim 12, Thomsen discloses associating a constraint with a key (§2.3) where the constraint must be satisfied before access to a computer resource governed by the key chain is granted (§2.3 ¶1).

24. Claims 1-35 are rejected under 35 U.S.C. 102(a) as being anticipated by printed publication "Napoleon Network Application Policy Environment" by Thomsen, O'Brien and Payne (**Thomsen**). Thomsen discloses using an application layer, semantic layers and a local layer (Fig. 2 & §2), encapsulating keys into key chains, and exporting the key chains to the next layer (§2 & Fig. 2), combining methods into handles, handles into keys and keys into key chains (Fig. 3), and adding constraints to the key chains at each layer (Fig. 4), assigning users to key chains (§2.3), using a user interface to manage the RBAC policy (§3) and translating the policy to the security mechanisms (§4).

25. Claims 1-4 & 32 rejected under 35 U.S.C. 102(a) as being anticipated by "The ARBAC97 Model for Role-Based Administration of Roles" by Sandhu et al. (**Sandhu**).

Regarding claim 1, 3 & 32, Sandhu discloses encapsulating security mechanism application specific information/permissions for each security mechanism/permission (p. 122, §5), wherein encapsulating includes forming a key/ability for each security mechanism/permission, combining keys/abilities to form key chains/abilities, encapsulating key chains/abilities as keys/abilities (p. 122, §5) and passing the key chain keys/abilities to another semantic layer/UP-Roles (p. 122, §5), defining the security policy/UP-Roles (p. 122, §5), wherein defining includes forming key chains from keys/abilities and associating users with key chains/abilities (p. 122, §5), translating the security policy/UP-Roles and exporting the translated security policy to the security mechanisms, and enforcing the security policy via the security mechanisms (p. 107, ¶5 & Fig. 1).

Regarding claim 2, Sandhu discloses distributed computer networks/enterprise-wide systems (p. 106, ¶4).

Regarding claim 4, Sandhu discloses UP-Roles, containing both abstracted abilities and permissions (p. 122, §5). If a new role is to be created, the next layer (abilities/users) is drilled to/accessed to combine the necessary elements.

### *Claim Rejections - 35 USC § 103*

26. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

27. Claims 5-10 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Sandhu**, as applied to claim 1 above, in further view of "Issues in the Design of Secure Authorization Service for Distributed Applications" by Varadharajan, Pato and Crall (**Crall**).

Regarding claim 5, Sandhu discloses a system, as described above, but lacks a graphical user interface. However, Crall teaches that a graphical user interface makes it easy for administrators to manage large numbers of users with consistent policies across applications (p. 874). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use a graphical user interface to define the security policy. One of ordinary skill in the art would have been motivated to perform such a modification to make it easy for administrators to manage large numbers of users with consistent policies across applications, as taught by Crall (p. 874).

Regarding claim 6-8, Sandhu discloses a plurality of security mechanisms/permissions, a plurality of semantic layers (UP-Roles, abilities, permissions) (p. 122, §5), wherein the first semantic layer combines keys/abilities, wherein each key encapsulates security mechanism application specific information for a security mechanism (permissions for resources) (p. 122, §5), wherein in multiple layers, keys are combined into key chains and exported to another semantic layer (permissions combined into abilities, abilities combined into additional abilities, combination abilities combined into UP-Roles). Sandhu lacks an explicit translator for translating the security policy to the security mechanisms and lacks a user interface. However, Crall discloses an "Authorization Server", which employs an interface to make it easy for administrators to manage users (p. 874). In disclosing the physical implementation that Sandhu lacks, Crall further discloses that authorization checks result from the security mechanisms/authorization mechanisms (p. 876, §2.4) when changes are made, translation occurs to keep the authorization database up to date (p. 878, ¶1). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to include a translator to translate the security policy to the security mechanisms and to include a user interface. One of ordinary skill in the art would have been motivated to perform such a modification to implement Sandhu's invention, in order to keep the authorization database up to date and to allow administrators to manage large groups of users, as taught by Crall (p. 874, p. 876, §2.4 & p. 878, ¶1).

Regarding claim 9, Sandhu discloses the semantic layers (role hierarchy) organized in a POSET/partial order to facilitate inheritance.

Regarding claim 10, Sandhu discloses that new key chains/abilities can be formed by any combinations of abilities and permissions (p. 122, §5), but lacks a user interface. However, Crall teaches that a graphical user interface makes it easy for administrators to manage large numbers of users with consistent policies across applications (p. 874). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use a graphical user interface to define the security policy. One of ordinary skill in the art would have been motivated to perform such a modification to make it easy for administrators to manage large numbers of users with consistent policies across applications, as taught by Crall (p. 874).

Regarding claims 11 & 13, Sandhu discloses a model comprising one or more semantic layers/roles for defining different security policies (p. 122, §5) and constraints (p. 108, ¶1) for each type of user, but lacks a tool for manipulating the model and lacks a translator for translating security policies from the model to security mechanisms in one or more computer resources. However, Crall discloses an "Authorization Server", which employs an interface to make it easy for administrators to manage users (p. 874). In disclosing the physical implementation that Sandhu lacks, Crall further discloses that authorization checks result from the security mechanisms/authorization mechanisms (p. 876, §2.4) when changes are made, translation occurs to keep the authorization database up to date (p. 878, ¶1). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to include a translator to translate the security policy to the security mechanisms and to include a tool for manipulating the model. One of ordinary skill in the art would have been motivated to perform such a modification to implement Sandhu's invention, in order to keep the authorization database up to date and to allow administrators to manage large groups of users, as taught by

Crall (p. 874, p. 876, §2.4 & p. 878, ¶1). As modified, Sandhu discloses enabling an administrator to encapsulate security mechanism application specific information for each security mechanism, wherein encapsulating includes forming a key/permission for each security mechanism/permission, combine keys to form key chains/abilities, encapsulate key chains/abilities as keys/abilities within two or more semantic layers (abilities, UP-roles), pass the key chain keys/abilities to other semantic layers (abilities->abilities, abilities->UP-roles, UP-roles->UP-roles), form user key chains/UP-roles from the key chain keys, and associate users with user key chains (UP-roles designated) (p. 122).

### *Conclusion*

28. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

29. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (571) 272-3841. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m.. The examiner can also be reached on alternate Fridays from 6:45 a.m. – 3:15 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached at (571) 272-3838.

**Any response to this action should be mailed to:**

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

**Or faxed to:**

(571) 273-8300
(for formal communications intended for entry)

**Or:**

(571) 273-3841 (Examiner's fax, for informal or draft communications, please label "PROPOSED" or "DRAFT")

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-2100.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

November 7, 2005
MJS

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100